

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DIRECTV, INC., a California corporation,

Plaintiff,

v.

David Annand,

Defendant.

No. 03-cv-12325 MLW

**DECLARATION OF JAMES
WHALEN**

I, James F. Whalen, declare the following:

1. My name is James F. Whalen. I am over twenty-one (21) years of age and reside in Los Angeles County, California. I am the Senior Director in DIRECTV's Office of Signal Integrity that is principally responsible for investigating reports of satellite piracy involving the DIRECTV satellite television system. I am familiar with the usual and customary practices involved in all aspects of DIRECTV's investigations of individuals and businesses suspected of illegally obtaining access to DIRECTV programming and the damages that illegal interception causes the company. I make this declaration based on personal knowledge and, if called to testify, could and would testify to the facts and opinions set forth herein.

2. As Senior Director in charge of the Office of Signal Integrity for DIRECTV, Inc., I am responsible for investigating reports of theft of DIRECTV's satellite signal. Over the past four (4) years I have led or overseen several hundred investigations of individuals and businesses engaged in the design, manufacture, distribution and sale of pirate Access

Cards and other devices intended to facilitate the unlawful reception and decryption of DIRECTV's satellite transmissions of television programming.

3. As Senior Director in charge of the Office of Signal Integrity, I have personally participated in the execution of numerous criminal search warrants. Law enforcement agencies frequently request that I accompany them on their searches to identify business records, illegal decryption equipment, computer files and other potential evidence of satellite signal theft. I have reviewed thousands of pages of banking, shipping, telephone, and other records seized from suspected satellite pirates, and have advised law enforcement personnel as to my opinions and conclusions regarding the contents of those records.

DIRECTV's Satellite Television System

4. DIRECTV is the nation's leading direct broadcast satellite system, delivering approximately 225 channels of digital entertainment and informational programming to approximately 14 million homes and businesses equipped with specialized DIRECTV receiving equipment. DIRECTV has invested billions of dollars to develop the United States' first high-power, direct broadcast satellite system.

5. DIRECTV encrypts – electronically scrambles – its satellite signal transmissions to provide for security and prevent unauthorized viewing of its television programming. DIRECTV offers its television programming to residential and business customers on a subscription and pay-per-view basis only. In order to receive and view DIRECTV satellite programming, each customer is required to obtain DIRECTV satellite hardware (including a small satellite dish and a DIRECTV integrated receiver/decoder (“IRD”) with a DIRECTV access card) and is required to establish an account with

DIRECTV. DIRECTV sells and distributes the DIRECTV satellite hardware necessary to receive DIRECTV programming.

6. Upon activation of the Access Card by DIRECTV, the customer can receive and view in a decrypted (i.e. unscrambled) format those channels to which the customer has subscribed or otherwise made arrangements to purchase from DIRECTV. Each DIRECTV access card contains an embedded microprocessor and uses smartcard technology to: (1) control which DIRECTV programming the IRD descrambles based on the programming package or other programming specifically purchased by the subscriber; and (2) capture and transmit to DIRECTV the subscriber's pay-per-view information (via a telephone modem in the IRD). Distributors of pirate access devices or illegally modified access cards routinely advised purchasers of piracy equipment not to plug their IRD units into a phone line to avoid a callback and to prevent detection by DIRECTV.

7. All programming transmitted by DIRECTV is digitized and compressed. The resulting signal is encrypted – electronically scrambled – by DIRECTV to prevent illegal and unauthorized reception. DIRECTV then transmits the signal to satellites located in stationary orbit approximately 22,300 miles above the earth. DIRECTV's satellites relay an encrypted television programming signal back to earth, where it can be received by homes and businesses equipped with DIRECTV satellite receiving hardware. This equipment includes several separate and distinct devices or components. The only authorized configuration of DIRECTV's satellite receiving equipment includes the following devices or components: 1) a mini-satellite dish; 2) a DIRECTV integrated receiver/decoder or IRD (a set top unit approximately the size of a VCR); 3) a DIRECTV

Access Card that works in conjunction with the IRD; and 4) cabling to connect the satellite dish, receiver, and viewing monitor.

8. DIRECTV offers several different satellite television subscription packages. DIRECTV offers 40 premium movie channels, including several Home Box Office®, Showtime, Cinemax, Movie Channel, Encore channels, the Family Pack™, and many local channels for many markets throughout the United States. DIRECTV offers several subscription packages ranging in price from \$36.99 per month for Total Choice to \$90.99 per month for Total Choice Premier with Local Channels.

9. DIRECTV also markets to individuals interested in specialized sports packages. DIRECTV offers subscriptions to specialized sporting packages, including NFL Sunday Ticket™, NBA League Pass™, NHL Center Ice™, MLB Extra Innings™, ESPN Game Plan™, ESPN Full Court™, MLS Direct Kick™, and Mega March Madness™. Each of these specialized sports packages can be purchased independent of the basic subscription fee.

10. DIRECTV also offers specialized one-time-viewing movies and events in the form of pay-per-view channels, numerous pay-per-view boxing and special event matches. The typical pay-per-view charges range from \$3.99 for each movie; to \$8.99 to \$10.99 for each Adult Program; and special sporting events such as a championship boxing match can cost as much as \$49 for each event.

11. DIRECTV incurs tremendous expense acquiring the rights to distribute all of this television programming and service. Furthermore, DIRECTV's revenues are principally derived from subscription fees related to its programming services and advertising revenues. Thus, DIRECTV has significant interests, commercial and otherwise,

in maintaining and securing the integrity of its programming and in prohibiting unauthorized reception of its satellite broadcast transmissions. For the above reasons, DIRECTV diligently protects its distribution rights.

DIRECTV'S ANTI-PIRACY EFFORTS

12. Addressing piracy is the job of several departments and many individual employees and independent contractors, experts and attorneys retained by DIRECTV. The Office of Signal Integrity, the engineering department, and the legal department are primarily responsible for DIRECTV's anti-piracy efforts.

13. DIRECTV has gone to great expense to create the Office of Signal Integrity and staff it with personnel to investigate the theft of DIRECTV's satellite programming services. In addition to the cost of a permanent, full-time investigative staff, DIRECTV has, on a case-by-case basis, contracted with private investigators to assist in its investigations into allegations of signal theft. The Office of Signal Integrity also supports law enforcement agencies such as the Federal Bureau of Investigation and state law enforcement agencies in their investigations of cases involving theft of satellite television services.

14. The availability of piracy devices has resulted in technical efforts by DIRECTV to address the piracy problem. One technical effort is to replace older, compromised Access Cards with new, secure cards. The costs associated with designing and manufacturing replacement access cards and sending those replacement cards to existing customers are substantial.

15. DIRECTV periodically transmitted electronic countermeasures ("ECMs"), which are electronic signals sent through the data stream to disable illegal access cards.

This requires the expenditure of funds to purchase sample illegal devices from the pirate marketplace for testing, and the devotion of engineering time to write the software for, test and implement the ECM. To date, DIRECTV has not quantified these expenditures, but they are significant.

16. In addition to the costs associated with the efforts mentioned above, DIRECTV pursues its anti-piracy efforts through civil litigation against satellite pirates. DIRECTV has filed hundreds of lawsuits against individuals and business entities in the United States, Canada and Mexico engaged in the business of designing, manufacturing and distributing pirate access devices designed for use with DIRECTV systems. Through these lawsuits, DIRECTV has also shut down hundreds of internet websites operating with the purpose of distributing illegal devices, software and instructions intended to be used with such devices.

17. DIRECTV also executes civil raids on individuals and entities involved in piracy resulting in the seizure of large inventories of illegal devices. Pursuant to the raids and lawsuits, DIRECTV also obtained various records that evidencing ongoing illegitimate enterprises engaged in the distribution of devices primarily designed for the unauthorized interception of DIRECTV's Satellite Programming.

18. DIRECTV created the End-User Development Group to pursue end-users of pirate devices and negotiate settlements of DIRECTV's claims against such individuals. The End-User Development Group has sent demand letters and negotiated settlements with tens of thousands of users of illegal devices. Because a pre-litigation settlement cannot be reached in every case, DIRECTV has filed lawsuits against thousands of end-users of illegal devices.

19. Each of the measures described above costs DIRECTV money that it would not have to spend were it not for piracy.

20. Since DIRECTV has acquired such a complete line-up of quality channels, movies, and specialized programs and sporting events, individuals go to great lengths to circumvent DIRECTV's encryption and security measures. The number of individuals involved in the manufacture and sale of illegal devices used to circumvent DIRECTV's encryption technology increased since DIRECTV began operations in 1994. In the fall of 1995, devices first appeared for pirating the DIRECTV satellite system. These devices initially consisted of circuit boards that operated in the place of valid DIRECTV Access Cards. Subsequently, satellite pirates succeeded in illegally modifying the Access Cards themselves to receive DIRECTV's satellite television programming without authorization by or payment to DIRECTV. Paralleling this evolution in pirate technology was the appearance of devices that were designed to facilitate the illegal modification of DIRECTV Access Cards.

21. An integral part of DIRECTV's anti-piracy program has been the periodic introduction of new generations of DIRECTV Access Cards, each built around a new microprocessor developed exclusively for the DIRECTV satellite system, as well as the periodic transmission of ECMs. The goal of both measures was to render obsolete existing pirate devices and to put satellite pirates to the task of starting all over again and attacking the new technology employed. DIRECTV has invested significant time and expense in these processes.

DIRECTV'S Losses and Other Damages Due to Piracy

22. The business of piracy can be a lucrative endeavor both for the large manufacturer and the small dealer. Records obtained pursuant to raids in Canada and in the United States show that pirates have generated substantial revenues from the distribution and manufacture of illegal access devices, often amounting to millions of dollars for an individual distributor of pirate devices. Obviously, there was a substantial black market for pirate access devices used in conjunction with DIRECTV systems, and DIRECTV has pursued all available avenues to curtail those sales.

23. Piracy itself has affected DIRECTV immeasurably. A considerable difference between pirates and paying customers relates to the way individuals obtain DIRECTV's pay-per-view movies and specialized programming. If a paying customer wants to view a pay-per-view program, he pays for the entire program regardless of whether or not he watches the entire program or changes the channel after five minutes. However, people who are viewing television programming for free have an unfettered ability to view parts of numerous programs without paying for a single one. Indeed, while a legitimate subscriber might spend \$4.00 to view one program during a two-hour period, a pirate can view programming with a much higher value during the same two hours. For example, DIRECTV typically has numerous pay-per-view movies playing at a given moment at an average cost of approximately \$4.00 per movie and adult programs at an average cost of approximately \$8.00.

24. Thus, an individual using one pirated DIRECTV access card would have access to over a million dollars in annual programming services and would not have had to pay for any of it. That figure includes the value of every pay-per-view movie even though the same movie is shown several times a day. Recognizing that not many will view one

movie more than once, DIRECTV has also calculated the value of all subscription packages and movies viewed only once. That value is well over \$150,000.00 annually. While DIRECTV has gone to significant efforts to acquire programming distribution rights from program providers, any loss of confidence by such providers in the security of DIRECTV's signal may affect DIRECTV's ability to obtain those rights in the future. DIRECTV has also calculated the value of programming purchased by the typical DIRECTV high-end legitimate customer (top 10% of subscribers to our Total Choice Premier package). This approach is based on the assumption that the typical user of a modified access card or other signal theft device would view at least the same amount of programming as the typical high-end paying customer. In fact, since there is no DIRECTV hardware or subscription costs associated with viewing programming, it seems more likely that the user of the illegal access device would make significantly greater use of DIRECTV's proprietary programming than would the honest subscriber who pays for each channel he uses. Those who invest hundreds of dollars in illegal devices and software can be expected to view a significant amount of television programming. Anecdotal information obtained by DIRECTV suggests that users of modified access cards are heavy consumers of sports subscriptions, pay-per-view movies and events (such as boxing matches), and adult programming.

25. The average monthly bill sent to the top 10% of DIRECTV's legitimate customers for the year 2003 was \$229.08. This included both subscription and pay-per-view charges. Assuming a user of a modified access card would view as much programming as a typical high-end paying customer, the annual value of programming stolen by such a user would be \$2,748.96, (12 x \$229.08). This is a conservative estimate of the value of

programming that was intercepted by Defendants since the use of a modified DIRECTV access card would provide access to all DIRECTV programming at no cost. This view does not address the value of programming unlawfully taken by Defendant, but focuses on what a legitimate subscriber might pay. A person with unlimited access to all programming is likely going to obtain a much greater benefit. As a result of analyzing these figures, it is relatively clear that the value of pirated services can easily amount to thousands of dollars annually.

26. Incremental increases in programming costs due to security concerns are directly related to satellite piracy. Moreover, the use of illegally modified access cards also adversely affects DIRECTV dealers in the United States who rely on commissions from the sale of DIRECTV programming. Because the use of a modified access card or other signal theft device allows the owner to obtain “free” DIRECTV programming, there is no need to subscribe to DIRECTV. The absence of subscriptions means that DIRECTV dealers do not receive commission checks. Similarly, dealers receive charge-backs on their pre-paid commissions if DIRECTV programming is not activated for the hardware sold by the dealers.

27. DIRECTV does not maintain records that would demonstrate the actual profit, if any, realized on the monthly fees paid by any individual subscriber. While the margin of “profit” is generally known with respect to particular subscription packages, this figure does not take into account the substantial investment costs in technology, including the fleet of satellites and the broadcast system itself, corporate overhead, subscriber acquisition costs (*i.e.*, sales commissions, equipment subsidies, marketing and advertising costs) and other expenses that would be relevant to a calculation of profit. Rather, it is

simply a gross comparison of the price paid for the particular programming by DIRECTV and the charge to the customer for a package that contains that particular programming. Furthermore, this type of programming cost information is very closely guarded, proprietary information that is the subject of extensive security measures and contractual confidentiality provisions. In the event the Court wishes to know this information in connection with this case, DIRECTV requests that an opportunity be given to submit information for strictly *in camera* inspection that would not become part of the public record.

28. In summary, DIRECTV encrypts its transmissions to provide security for and prevent unauthorized viewing of that programming. DIRECTV provides subscribers with access cards specifically developed for the DIRECTV system. Each DIRECTV access card contains a microprocessor and uses smartcard technology to control the subscriber's access to DIRECTV's programming consistent with the programming purchased by the subscriber.

Evidence of the Defendant's Purchases of Devices Designed for Piracy

29. On or about November 16, 2001, United States District Judge Dean D. Pregerson granted DIRECTV's application for a Temporary Restraining Order, Impoundment Order, and Order to Show Cause against Scott Gray and Sandra Gray, d/b/a/ The Computer Shanty, among others. Pursuant to the Order, on or about December 1, 2001, DIRECTV executed a civil seizure, with the assistance of the United States Marshals Service, upon The Computer Shanty, an Internet seller of Pirate Access Devices. Shanty's business enterprise focused on distributing satellite signal theft devices, primarily designed for the surreptitious interception of satellite communications broadcast by DIRECTV,

through the website Shanty.com.

30. The seizure revealed information related to Shanty and its customers. Pursuant to the seizure and the litigation against Shanty and its owners, DIRECTV obtained various business records evidencing the ongoing illegitimate enterprise, including orders, invoices, electronic communications, and shipping documentation. Several months following the seizure, on or about September 5, 2002, DIRECTV obtained additional customer purchase records, by means of a third-party subpoena served upon Network1 Financial Corporation, the credit card processing company used by The Computer Shanty. Each record confirmed the existence of a distribution source for the country-wide transmission of devices primarily designed for the unauthorized interception of DIRECTV's Satellite Programming. Those records evidence Annand's purchase of an ULProX SU2 Super Unlooper and a DualPro WTX Ultimate Unlooper Programmer from The Computer Shanty on or about January 25, 2001.

31. The ULProX SU 2 Super Unlooper purchased by the Defendant is designed and/or marketed to be used to permit the unauthorized interception of DIRECTV's signals. An Unlooper is a programming device designed to break a looping software cycle to a modified Access Card. Specifically, the "Unlooper" is designed to repair illegally modified DIRECTV access cards that were rendered inoperable by DIRECTV's electronic security measures commonly referred to as Electronic Counter Measures or "ECMs." An ECM is sent electronically by DIRECTV by satellite and is intended to disable illegally modified DIRECTV access cards that are being used to receive DIRECTV programming without authorization. Once these cards are disabled, (or are "looped" as the condition is known), they no longer allow free viewing of DIRECTV programming without the additional use of

other electronic devices or equipment to return the illegal functionality. Individuals interested in continuing the illegal receipt of DIRECTV programming use an unlooper to restore functionality to a disabled card, thus allowing the access card to once again receive DIRECTV programming for free. Effectively, the unlooper tricks the DIRECTV access card into allowing access to the memory on the access card so that the card can be rewritten after it has been “looped” or disabled by an ECM. An unlooper has the specific ability to manipulate the voltage and clock of the DIRECTV access card in a manner that allows the user of the unlooper to restore functionality to a DIRECTV access card. The primary application of the clock/voltage manipulation capability (also known as “glitching”) is to illegally modify, or attempt to illegally modify, a DIRECTV access card. Indeed, the term “unlooper” was coined specifically to refer to devices that restore functionality to “looped” pirated DIRECTV access cards.

32. The DualPro WTX Ultimate Unlooper Programmer purchased by Defendant is a device that has the combined functionality of a programmer and an unlooper. The device is primarily designed to assist in the surreptitious interception of DIRECTV satellite programming without authorization by or payment to DIRECTV. As a programmer, the device is used to permit the illegal programming of—writing of code to—valid DIRECTV Access Cards for the purpose of obtaining access to DIRECTV Satellite Programming without paying DIRECTV. By way of example, the programmer is used (i) to “clone” Access Cards, enabling an unauthorized (or inactivated) Access Card to decrypt the same programming as a particular authorized (or activated) Access Card; or (ii) to program Access Cards to receive all DIRECTV programming, including pay-per-view events, without payment to DIRECTV.

33. It is common for DIRECTV signal pirates to maintain a level of legitimate DIRECTV service while engaging in piracy of DIRECTV television programming. Indeed, a substantial portion of signal piracy investigated or discovered by DIRECTV involves individuals who are DIRECTV subscribers, or have been in the past.

DIRECTV Account History

34. DIRECTV's satellite television signal is encrypted – electronically scrambled – to prevent unauthorized reception. In order to receive and view DIRECTV signals, a person needs certain hardware, including a DIRECTV satellite dish, a DIRECTV integrated receiver/decoder (or “IRD”), and a DIRECTV Access Card. Paying customers of DIRECTV obtain this equipment, and the connecting cables and cords, at highly subsidized prices or for free.

35. Defendant Annand purchased DIRECTV satellite equipment from Circuit City, and on or about June 7, 1998, created DIRECTV Account Number 004819086. He maintained that subscription purchasing a considerable amount of adult paper views until his account was disconnected on December 11, 1999. Thus, Defendant is shown to possess all DIRECTV satellite equipment necessary to receive DIRECTV satellite programming without authorization, when used together with the Pirate Access Devices he purchased.

EVIDENCE OF DEFENDANT ANNAND'S UNAUTHORIZED ACCESS TO DIRECTV AND ACTIVITY IN INTERNET PIRACY COMMUNITY

36. DIRECTV has been able to locate evidence on the internet, that Defendant Annand, using the username “Dannand,” along with the email address “dca9971@msn.com” visited and posted messages relating to the piracy of DIRECTV programming on websites and/or usenet forums.

Websites and Usenet Groups Generally

37. Pirates of DIRECTV's signal utilize a number of websites and usenet forums for the dissemination and exchange of information pertaining to piracy technology and satellite piracy generally. The "forum" websites and usenet groups typically include chat rooms where users can "post" information on such matters as the latest ECMs launched by DIRECTV and software "patches" and "fixes" to resurrect illegally-modified DIRECTV Access Cards that have been disabled by ECMs.;

38. In some cases, the forum websites or usenet groups do not sell any piracy technology themselves. They rather provide information and links to other piracy websites that sell piracy devices, piracy software, and related services to permit consumers to unlawfully obtain DIRECTV's programming. It is typical for forum sites and groups to receive advertising revenue from other piracy websites and vendors that place advertisements or links on them.

39. Forum sites and usenet groups typically require considerable data storage capacity because they have to store numerous messages posted by users and make those messages available to others. For this reason, forum sites and groups store data on secure, high capacity servers located at internet service providers or "host" facilities. The servers typically contain the forum sites and groups, including all of the pages of the site and databases with member and customer records, and electronic data pertaining to the websites business.

The Initial Investigation

40. DIRECTV has investigated numerous websites and usenet groups devoted to piracy, including but not limited to www.pirateden.com ("Pirate Den"), www.dssworld.org ("DSS World"), www.dsschat.com ("DSS Chat") and www.decodernews.com ("Decoder News"), to determine the identity of the persons behind them.

41. DIRECTV's investigation revealed that the "Pirate Den", was primarily devoted to exchanging information and/or tools for the piracy of DIRECTV satellite signals.

42. The investigation also revealed that a number of piracy websites use a number of "meta tags" or "meta names," which are "key words" embedded in the source code for the pages of the web sites, which attract Internet traffic through the use of specific key word searches. These meta names included: "dss hack," "test cards," "DirecTV," "dssunderground," "test card," "satellite hack cards," "3m cards," "4m cards," "3m," "4m," "t3," "t3 cards," "combo cards," "ddt cards," "smart cards," and "hack cards." These meta tags refer to known piracy terms, devices, cards, and software for the reprogramming of DIRECTV Access Cards.

43. The Pirate Den Web Site promoted Pirate Den as:

"Pirates Den...the site of choice for the true DSS [i.e., DIRECTV] satellite hobbyist. For well over 5 years now, we have been providing un-biased news and information on the Digital Satellite Underground..."

44. In the "Founding Principles" page of the Pirate Den Web Site, the Pirate Den stated:

"Shortly after its release in 1995, the technology that enabled people to "Test" or "Pirate" the Directv signal was released in

Canada, and it soon became apparent the eyes of the law, it was considered just as illegal for a Canadian resident to pay for a legitimate subscription via the "Grey Market" as it was to "pirate it"...

Hobbyists are those that generally possess an avid interest in the industry. They consider "Free Tv" to be a natural by-product of their hobby...The Pirates Den is the result of over 5 years of personal effort into developing a site that caters mostly to the "Hobbyists", including a vast library of knowledge, news, FAQ's, forums and much more..."

45. Pirate Den offered the following services through its Web Site:
- a. "click through" banner advertising links to "Pirates Den Top 100" web sites selling Piracy Technology and related services, which record thousands of "hits" for users who have accessed these sites through Pirates' Den;
 - b. "ECM Analysis" which provides listings of software programming code for ECMs launched by DIRECTV with commentary for advanced users and programmers describing how specific ECMs work;
 - c. a free public "DSS Chat Discussion Forum" which is described as "one of the largest and most popular discussion forums of its kind on the Internet, with over 130,000 registered posters" and which "no other satellite forum...can match";
 - d. a "Members Area" forum which "includes everything you need to become a knowledgeable veteran" and which offers the benefit of guaranteed access "during extremely peak times, such as an ECM, [when] our discussion forum can become temporarily overwhelmed with visitors";
 - e. information on the current status of DIRECTV Access Cards (H Cards, HU Cards, and P4 Cards) and "ECM Activity";
 - f. information on "Test Cards" and "ECMs";

- g. product reviews for such Piracy Technology as emulators, loaders, bootloaders, and unloopers;
- h. links to industry-related sites including sites with names such as DSS Hideaway, DSS Underground, DSS Tester, DSS Ware and Hack-this.com; and
- i. "DSS News Reports" on current DIRECTV enforcement activities (including ECMs, Piracy Technology devices which DIRECTV is targeting, and litigation by DIRECTV against pirates), information on software patches for DIRECTV Access Cards, and changes made by DIRECTV to its signal datastream.

46. The "Pirates Den Top 100" web sites collectively advertised practically every kind of Piracy Technology and included such sites, products and services as:

- 1. *scriptsforsell.com* ("scripts for sell," the best private 3M software scripts around);
- 2. *card cracker* (DIRECTV Access Card services, 3M scripts support);
- 3. *Hufiles.com* (HU card unloopers, free software);
- 4. *DSSfileshucards.com* (HU card loaders, HU files, HU software, HU instructions/tutorials);
- 5. *Access Card Canada* (private 3M service);
- 6. *DSS storm* (Mikobu III loaders);
- 7. *HU card-fix* (private HU scripts);
- 8. *HU fix Canada* (satellite 3Ms); and
- 9. *DSSHUpros.net* (private scripts, P4 cards).

47. The Pirate Den Web Site had a page entitled "Site Advertisers" which revealed that the Pirate Defendants received revenues, fees, and other consideration from the operation of the Web Sites. The Pirate Defendants indicated, "Our advertising rates are USD \$200.00 a month for a rotating 468 x 60 pixel banner at the top of the forums and also

on the main site” and “a limited number of static banners available...for...USD \$1000.00 a month.” The Web Sites revealed that Pirate Den had over 100 advertisers.

Results of DIRECTV's Investigation of Defendant's Websites Activity

48. Pursuant to DIRECTV's investigation and lawsuits against vendors of piracy technology, DIRECTV came into possession of a substantial body of records, including email communications, subscription invoices, credit card receipts and other records. Those records indicate that Defendant Annand joined Pirate Den's web site on or about January 20, 2001.

DAMAGES TO DIRECTV

49. By acquiring and using the above-referenced device, Mr. Annand had unencrypted access to every program transmitted by DIRECTV at all times. He had the ability to view any or all of DIRECTV's 225 programming channels, 24 hours per day. Several of these channels offer programming on a pay-per-view basis, which rebroadcasts several times a day. An individual using one pirated access card has access to over a million dollars worth of programming services annually. Obviously, even the most avid DIRECTV consumer could not possibly watch all available programming, all day every day. Assuming then, that each pay-per-view event is watched only once, the value of subscription and movies viewed only once is approximately \$166,000.

50. DIRECTV admittedly has no subscribers who generate such a bill for its services. However, DIRECTV estimates that the average signal hacker would have substantially higher viewing habits than the typical “high-end” subscriber. The average monthly bill sent to the top 10 per cent of DIRECTV's legitimate customers in 2003 was

\$229.08. This included both subscription and pay-per-view charges. Assuming a user of a modified access card would view as much programming as a typical high-end paying customer, the annual value of programming stolen by such a user would be \$2,748.96.

51. Making the generous assumption that Mr. Annand used only the amount of DIRECTV programming with a hacked access card as the typical high-end user, the above-referenced device enabled him to receive at least 39 months of programming, (from purchase of the Unlooper device in January 2001 until late April 2004 when DIRECTV shutdown its P3 data stream) valued at \$8,934.12.

52. Based upon the particular circumstances of this case, it is also likely and reasonable to conclude that the Defendant was already receiving DIRECTV programming without authorization or payment via use of an illegally-modified Access Card at least before Black Sunday in January 2001.

53. Notwithstanding the actual cost of stolen programming, the cost of piracy to DIRECTV is immeasurable. DIRECTV has made significant efforts to acquire certain programming distribution rights from program providers, the confidence of whom is affected by the security of DIRECTV's signals. Efforts, such as the Defendant's, to continuously circumvent DIRECTV's satellite security may affect DIRECTV's ability to obtain these programming rights in the future as they are periodically renewed and renegotiated.

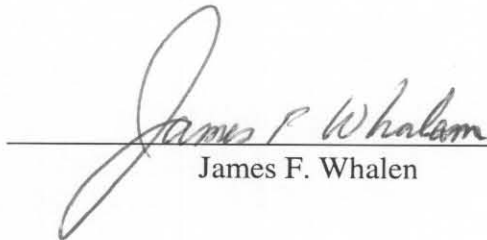
54. Incremental increases in programming costs due to security concerns are also directly related to piracy. Moreover, the use of illegally modified Access Cards

adversely affects DIRECTV dealers in the United States who rely on commissions from the sale of DIRECTV programming.

55. Based upon this information, DIRECTV sought and should be entitled to a significant statutory damage award for the unauthorized interception of signals 47 U.S.C. § 605(a) as alleged in the pending Motion for Default Judgment against Defendant.

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct.

DATED: August 12, 2005


James F. Whalen